Franchise Tax Board

SUMMARY ANALYSIS OF AMENDED BILL

Author: Jones, et al. Analyst: Deborah Barrett Bill Number: AB 1779

Related Bills: See prior Analysis Telephone: 845-4301 Amended Date: June 9, 2008

Attorney: Patrick Kusiak Sponsor:

SUBJECT: State Agencies Notify California Residents Of Breach In Security Data/if Substitute Notice Is Utilized, Provide to Office Of Privacy

_____ DEPARTMENT AMENDMENTS ACCEPTED. Amendments reflect suggestions of previous analysis of bill as introduced/amended _____.

_____ AMENDMENTS IMPACT REVENUE. A new revenue estimate is provided.

__X__ AMENDMENTS DID NOT RESOLVE THE DEPARTMENTS CONCERNS stated in the previous analysis of bill as introduced January 15, 2008.

_____ FURTHER AMENDMENTS NECESSARY.

_____ DEPARTMENT POSITION CHANGED TO _____.

__X__ REMAINDER OF PREVIOUS ANALYSIS OF BILL AS INTRODUCED January 15, 2008, STILL APPLIES.

_____ OTHER – See comments below.

SUMMARY

This bill would prohibit a state agency from retaining payment related data and would require that a state agency provide the Office of Information Security and Privacy Protection (OISPP) with a copy of the notice sent to California residents when a breach of security of a system containing personal information has occurred.

SUMMARY OF AMENDMENTS

The June 9, 2008, amendments would do the following:

- Prohibit the retention of payment related data when accepting a credit card, debit card, or other device in the sales of goods or services by a state agency.
- Prohibit the transfer of payment related data over open public networks unless the data is encrypted as specified.
- Defines and prohibits the retention of sensitive authentication data.
- Require that when a state agency provides notice of a breach of security to a California resident, to also send notice of the breach with specified information to the owner or licensee of the information.

Board Position:			Asst. Legislative Director	Date
_____ S	_____ NA	_____ NP		
_____ SA	_____ O	_____ NAR	Patrice Gau-Johnson	6/19/08
_____ N	_____ OUA	__X__ PENDING		

The June 9, 2008, amendments did not resolve the "Policy Concern" identified in the department's analysis of the bill as introduced January 15, 2008, and is repeated below for convenience. As a result of the June 9, 2008, amendments, a new "Implementation Consideration" has been identified and is discussed in the analysis below. Other than the preceding referenced changes made and the revisions to the "This Bill" and "Program Background" discussions, the remainder of the department's analysis of the bill as introduced January 15, 2008, still applies.

POSITION

Pending.

THIS BILL

This bill would prohibit, with certain exceptions, a person, business, or state agency that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device from storing payment related data, except as specified.

This bill would also prohibit the following:

- Storage of sensitive authentication data, as defined, subsequent to authorization,
- Storage of any payment related data that is not needed for business, legal, or regulatory purposes,
- Retention of the primary account number unless retained in a manner consistent with other provisions of the bill and in a form that is unreadable and unusable by unauthorized persons anywhere it is stored,
- Sending payment related data across any open public network unless the data is encrypted using strong cryptography and security, and
- Allowing access to payment related data by any individual whose job does not require that access.

Sensitive authentication data includes, but is not limited to, all of the following:

- The full contents of any data track from a payment card or other payment device
- The card verification code or any value used to verify transactions when the payment device is not present
- The personal identification number (PIN) or the encrypted PIN block

The provisions of this bill are not applicable to financial institutions that are compliant with federal regulations relating to disclosure of nonpublic information if subject to compliance oversight by a state or federal regulatory agency with respect to those regulations.

This bill would require agencies subject to the payment related data restrictions to notify the owners or licensees of the data if an unauthorized person breaches the system containing that data. This bill would provide that if notice is required, the agency whose system was breached is liable to the owner or licensee of the information for the reimbursement of actual costs of providing notice to consumers regarding the breach of the security of the system. If the agency processed more than six million payment card transactions per year, the agency is additionally liable to the owner or licensee of the information for the actual costs of reissuing the credit card, debit card, or other device not to exceed the amount of fifteen dollars per reissued credit card, debit card, or other payment device. If an agency can demonstrate that it complies with the payment related data restrictions of this bill, the agency is excused from reimbursement liability.

This bill would require notice to the owners or licensees of the payment related data to comply with certain requirements and would specify the type of information to be included in the notice.

A law enforcement agency may delay notice if it determines that notice will impede a criminal investigation. Notice in those circumstances would be made after a law enforcement agency determines that the notice would not impede the criminal investigation.

This bill would require that if substitute notice as authorized is provided, the OISPP must also be notified.

The provisions of this bill would not apply to FTB because the majority of FTB's transactions with taxpayers are payments of tax obligations, rather than purchases of goods or services. In addition, because the bill would make the requirement to notify owners or licensees of data in the event of a security breach conditioned upon being subject to the retention of payment related data requirements, these requirements in the bill would also not apply to FTB.

IMPLEMENTATION CONSIDERATIONS

It is not clear that the provisions of this bill are applicable to FTB because while taxpayers may purchase some items from the department, such as the Package X, the majority of FTB's transactions with taxpayers are not for goods or services but for payment of tax liabilities. The author may want to specify agencies that receive payments for purposes other than goods and services, such as for payment of obligations, to prevent any confusion about which agencies are intended to be included in the provisions of the bill.

PROGRAM BACKGROUND

FTB maintains a data retention policy for personal information that includes return information, including payment related data. Retention time frames vary from no less than the minimum amount of time required by law, to seven years from the later of the original due date of the income tax return, or the date the original, or an amended tax return was filed.

Additionally, FTB does not currently accept debit card payment transactions, unless the debit cards can be used interchangeably as credit cards. The other electronic payment option offered by the department is Web Pay. Web Pay is an online application that can be used to make electronic withdrawals from taxpayers' checking or savings accounts to pay their personal income tax. The payment can be scheduled up to one year in advance. Credit card payments are accepted for tax payments but are not currently available for use in the non-tax debt programs the department administers.

ARGUMENTS/POLICY CONCERNS

Because current State Information Management Manual instructions require state agencies that maintain systems containing personal information to provide an Incident Report to OISPP within ten days of the incident, the similar provisions of this bill, as they relate to state agencies, are duplicative.

LEGISLATIVE STAFF CONTACT

Legislative Analyst
Deborah Barrett
(916) 845-4301
Deborah.barrett@ftb.ca.gov

Revenue Manager
Rebecca Schlussler
(916) 845-5986
rebecca.schlussler@ftb.ca.gov

Asst. Legislative Director
Patrice Gau-Johnson
(916) 845-5521
Patrice.Gau-Johnson@ftb.ca.gov